Audit Report

OFFICE OF THE INSPECTOR GENERAL

APPLICATION CONTROLS OVER THE DEFENSE JOINT MILITARY PAY SYSTEM RESERVE COMPONENT

Report No. 97-203   August 13, 1997

This special version of the report has been revised to omit unclassified sensitive information pertaining to the security and administration of a major pay system of the DoD.

Department of Defense

1999 1013 142

AQI00-01- 0047

Additional Copies

To obtain additional copies of this audit report, contact the Secondary Reports Distribution Unit of the Analysis, Planning, and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or FAX (703) 604-8932.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Planning and Coordination Branch of the Analysis, Planning, and Technical Support Directorate at (703) 604-8939 (DSN 664-8939) or FAX (703) 604-8932. Ideas and requests can also be mailed to:

> OAIG-AUD (ATTN: APTS Audit Suggestions)
> Inspector General, Department of Defense
> 400 Army Navy Drive (Room 801)
> Arlington, Virginia 22202-2884

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@DODIG.OSD.MIL; or by writing to the Defense Hotline, The Pentagon, Washington, D.C. 20301-1900. The identity of each writer and caller is fully protected.

Acronyms*

AIS	Automated Information System
CICS	Customer Information and Control System
COP	Component of Pay
DAA	Designated Approving Authority
DFAS	Defense Finance and Accounting Service
DJMS	Defense Joint Military Pay System
DJMS-RC	Defense Joint Military Pay System Reserve Component
DMC	Defense Megacenter
IG	Inspector General
ISO	Information Security Officer
ISSO	Information System Security Officer
MMPA	Master Military Pay Account

*Sensitive computer security information deleted (DoD 5400.7-R).

August 13, 1997

MEMORANDUM FOR DIRECTOR, DEFENSE FINANCE AND ACCOUNTING
SERVICE
DIRECTOR, DEFENSE INFORMATION SYSTEMS
AGENCY

SUBJECT: Audit Report on Application Controls Over the Defense Joint Military Pay
System Reserve Component (Report No. 97-203)

We are providing this final report for review and comment. This audit was
requested by the Director, Defense Finance and Accounting Service Denver Center,
Denver, Colorado. We considered management comments on a draft of this report
when preparing the final report.

DoD Directive 7650.3 requires that all recommendations be resolved promptly.
The Defense Information Systems Agency comments conformed to the requirements of
DoD Directive 7650.3; therefore, additional comments are not required from that
organization. The Defense Finance and Accounting Service comments were partially
responsive. We request additional comments from the Defense Finance and
Accounting Service on Recommendations B.3.a. and B.3.b. by October 14, 1997.
Specific requirements for additional management comments are stated in Part I of the
report.

We appreciate the courtesies extended to our audit staff. Questions on the audit
should be directed to Mr. David C. Funk, Audit Program Director, at (303) 676-7445
(DSN 926-7445), or Mr. W. Andy Cooley, Audit Project Manager, at (303) 676-7393
(DSN 926-7393). See Appendix C for the report distribution. The audit team
members are listed inside the back cover.

David K. Steensma
Deputy Assistant Inspector General
for Auditing

**This special version of the report has been revised to omit unclassified sensitive
information pertaining to the security and administration of a major pay system
of the DoD.**

Office of the Inspector General, DoD

Report No. 97-203
(Project No. 6FD-2015)

August 13, 1997

Application Controls Over
the Defense Joint Military Pay System
Reserve Component

Executive Summary

Introduction. This audit was requested by the Director, Defense Finance and Accounting Service Denver Center, Denver, Colorado. The audit focused on controls over the Reserve component of the military pay application known as the Defense Joint Military Pay System. A prior audit evaluated security controls for the active-duty component of this application. In FY 1996, the Defense Joint Military Pay System Reserve Component paid $3.7 billion to Reserve and National Guard members of the Army and Air Force. This payroll application was managed by the Defense Finance and Accounting Service centers at Indianapolis, Indiana, and Denver, Colorado. Computer programming support was provided by the Defense Finance and Accounting Service, Financial Systems Organization, Directorates for Software Engineering-Military Pay, in Indianapolis and Denver. The Defense Information Systems Agency, Defense Megacenter-Denver, provided computer support.

Audit Objectives. The primary audit objective was to determine whether application and security software controls of the Defense Joint Military Pay System Reserve Component adequately safeguarded the data integrity of payroll records used to pay Army and Air Force Reserve and National Guard personnel. In addition, we also evaluated the effectiveness of applicable management controls.

Audit Results. Opportunities existed for improving application and computer security controls over the Defense Joint Military Pay System Reserve Component application. The results of this audit are summarized below and are detailed in Part I of the report.

o Data input and processing controls needed improvement. As a result, Army and Air Force members could be and, in some instances, were paid in excess of the allowable amount for pay entitlements and for entitlements that they were not authorized to receive. Because of inadequate input and processing controls, the potential existed for even greater overpayments and unauthorized receipt of payments than were discovered during the audit. Corrective action was initiated during the audit to automate entitlements and develop system edits (controls), report unreasonable * , and correct premature * (Finding A).

---

*Sensitive computer security information deleted (DoD 5400.7-R).

\

manipulate application resources without detection, jeopardizing the integrity of Army and Air Force pay data. When brought to management's attention, corrective actions were taken, but additional improvements are required (Finding B).

See Appendix A for details on the management control program.

Summary of Recommendations. We recommend that changes be made to the Defense Joint Military Pay System Reserve Component to add consistency and limit checks over entitlement payments and to strengthen controls over generic components of pay and *   transactions. We also recommend improvements in defining the security control structure for the Defense Joint Military Pay System and controlling access to its sensitive resources.

Management Comments. The Defense Finance and Accounting Service concurred with five recommendations, stating that systemic changes will be implemented to include consistency checks for *   and to create unique components of pay for all current training pay entitlements. In addition, the use of the generic components of pay will be identified as a new material weakness. The capability to monitor the use of the generic components of pay will be added to the pay system. Likewise, changes to the Reserve input systems will be implemented to require a memorandum entry for all transactions using the generic components of pay. Procedures have been established to request system access authorizations through the coordinating security officer.

The Defense Finance and Accounting Service partially concurred with two other recommendations, agreeing to assign the appropriate sensitive position designation and obtain background investigations for personnel in these positions in accordance with DoD policy. Management disagreed, however, that the Director, Defense Finance and Accounting Service, should be provided written assurance that DoD 5200.2-R criteria have been met.

The Defense Information Systems Agency concurred with the recommendations and implemented or planned adequate corrective action.

Audit Response. Management comments were partially responsive. We disagree with the rationale used by the Defense Finance and Accounting Service in its comments to two recommendations. We do not believe that relying on current organizational forms and amending the organization's regulation will ensure that the requirements of DoD 5200.2-R are satisfied. Therefore, we ask that management reconsider its position on those two recommendations. Comments by the Defense Information Systems Agency were fully responsive. Therefore, additional comments are not required.

See Part I for management comments and our responses and Part III for the complete text of management comments. We request that the Defense Finance and Accounting Service provide comments by October 14, 1997.

---

*Sensitive computer security information deleted (DoD 5400.7-R).

Table of Contents

Part I - Audit Results

Audit Background

System Overview. The Defense Joint Military Pay System (DJMS) is large, complex, and by every measure, one of the most sensitive administrative computer applications in the Department of Defense. During FY 1996, DJMS processed payroll transactions valued at over $19 billion for active-duty and $3.7 billion for Reserve and National Guard members of the Army and the Air Force. DJMS payroll processing is divided into two distinct components:

    o the active-duty component used to pay active-duty members of the Army and Air Force, and

    o the Reserve component (DJMS-RC) used to pay Reserve and National Guard members.

In this report, the term "DJMS Army" refers to the Army active-duty and Reserve components of DJMS. The term "DJMS Air Force" refers to the Air Force active-duty and Reserve components of DJMS.

This audit focused on application controls for DJMS-RC and included security software controls for the DJMS Army and Air Force active-duty and Reserve components. A prior audit evaluated the DJMS Army and Air Force active-duty component (see Appendix B). Both audits were requested by the Director, Defense Finance and Accounting Service (DFAS) Denver Center, Denver, Colorado.

Supporting Organizations. Identified as a Headquarters, DFAS, automated information system (AIS), DJMS is supported by three DFAS organizations and the Defense Information Systems Agency.

    DFAS Denver Center. The Directorate of Military Pay at the Denver Center (DJMS Denver) is responsible for the integrity of the military pay data for the Air Force and all three military academies. In addition, DJMS Denver is responsible for the core pay software that supported DJMS as a whole and the related software specific to the Air Force and military academies.

    DFAS Indianapolis Center. The Directorate of Military Pay at the Indianapolis Center (DJMS Indianapolis) is responsible for the integrity of the military pay data for the Army. DJMS Indianapolis is also responsible for the software specific to Army military pay and the software bridges and interfaces necessary for DJMS Army to interact with the core software.

    Software Engineering Directorate. Software development, design, testing, and other central design support for DJMS is provided by the DFAS,

Financial Systems Organization, Directorates for Software Engineering-Military Pay in Denver and Indianapolis (referred to in this report as the Software Engineering Directorate).

Defense Megacenter (DMC)-Denver. DJMS software is installed on mainframe computers operated by the Defense Information Systems Agency, Western Hemisphere, DMC-Denver.

Master Military Pay Account (MMPA). The heart of DJMS is a computer file containing a MMPA for every active-duty, Reserve, and National Guard member of the Army and Air Force. All data flow into and update the MMPA files. The output is produced either from data shown in the file or from daily transaction processing. The MMPA record contains all information on the member's entitlement, deductions, allotments, *   , payments, status, leave, and payroll history for the past year. All data concerning the member that is, has, or will determine pay or relate to pay distribution are contained in the member's MMPA.

All MMPAs are maintained by and updated at either DJMS Indianapolis or DJMS Denver. Both DFAS centers serve as a central site activity for collecting and processing input from several sources, such as the Army and Air Force Reserve and National Guard Payroll Offices.

Security Software. Computer Associates International, Inc. (CA), Top Secret security software is used to control access to all DJMS Army and Air Force resources, including individual access capabilities. This security software provides system security and control over DJMS software, data, and data communications. It identifies the users allowed access to the computer systems and defines the resources such users are authorized to access. When properly implemented, CA-Top Secret security software ensures conformance with DoD security requirements.

Audit Objectives

The primary objective of our audit was to determine whether DJMS-RC application and security software controls adequately safeguarded the data integrity of payroll records used to pay Army and Air Force Reserve and National Guard personnel. In addition, we evaluated the effectiveness of applicable management controls.

See Appendix A for a discussion of the scope and methodology and the results of our review of the management control program. See Appendix B for a discussion of prior audits and other reviews related to our audit objectives.

---

*Sensitive computer security information deleted (DoD 5400.7-R).

Finding A. Data Input, Processing, and Output Controls

While adequate output controls existed, DJMS-RC data input and processing controls needed improvement. Specifically, data input controls did not include limit checks[1] in processing five entitlement payments and *   . Also, data processing controls needed strengthening to provide for:

  o consistency checking[2] in processing entitlement payments,

  o adequate control and oversight of the use of and audit trails for generic components of pay (COPs), and

  o better control over *   that bypassed system edits.

These controls were inadequate because DJMS-RC programming did not include certain automated tests and edits to validate data inputs or to check the consistency of data during computer processing. As a result, military members were paid $25,000 in excess of the allowable amount for *   , and enlisted members received * to which they were not authorized. In addition, the potential existed for even greater overpayments and unauthorized receipt of payments than were discovered during the audit. These inadequate input and processing controls over DJMS-RC entitlement payments constituted a material management control weakness. DJMS Denver initiated corrective action to automate entitlements and develop system edits (controls), report unreasonable *   , and correct premature transaction posting to the *   . However, these changes were not completed during the audit.

---

[1]Limit checks during computer processing automatically test specified data fields against defined high- or low-value limits for acceptability before processing further.

[2]Consistency checking is designed to automatically compare certain values in the same or different records to determine accuracy and reasonableness.

*Sensitive computer security information deleted (DoD 5400.7-R).

Application Controls

Computer Controls. In computer operations, application controls consist of data input, processing, and output controls. Input controls help ensure the integrity of data during conversion into machine-readable format and entry into the application. Processing controls help verify the integrity of inputs processed by the computer so that no data are added, lost, or altered during processing. Data output controls help safeguard the integrity of reports generated by the computer and ensure reports are correctly distributed in a timely manner.

Audit Focus. As noted in Appendix A, the audit evaluated application controls over five pay entitlements. These entitlements were selected for review based on the high-dollar amount expended for the entitlement or other factors that might present a risk to the integrity of the military pay data. Entitlements were selected based on DJMS-RC Army and Air Force data available at the time of selection.

*

*

*

*Sensitive computer security information deleted (DoD 5400.7-R).

The audit also evaluated application controls over three generic components of pay and *   .

As detailed in Appendix A, the audit was accomplished by establishing accounts and submitting transactions to the DJMS Army and Air Force test environments. Actual DJMS-RC payroll transactions during August 1996 were examined on a limited basis to quantify the impact of application control weaknesses identified by the audit. Subsequent output reports were reviewed.

Input Controls

Limit Checks. DJMS-RC data input controls over five pay entitlements and *   needed improvement.   Specifically, DJMS-RC programming did not include automated maximum limit checks on transactions used to pay *

*

*

**

*

---

*Sensitive computer security information deleted (DoD 5400.7-R).

**Sensitive computer security footnote information deleted (DoD 5400.7-R).

*

*

*

*

*

*Sensitive computer security information deleted (DoD 5400.7-R).

7

*

*

*

*

Corrective Actions. DJMS Denver took some corrective actions during the audit.

o Management submitted system change request *   to the DJMS change control board, chaired by the DJMS Program Manager, to automate entitlements and develop * edits for maximum daily rates for pay transactions. The board approved the system change in December 1996; however, an implementation date had not been set.

o Management   was   also   aware   that   unreasonable   rates for *   existed.   DJMS   Denver   developed   system   change request *   to provide a report to commanders on these *   and their *   rates. This system change was approved by the change control board in May 1996 and is scheduled for implementation to DJMS production processing in April 1997.

As a result of management's actions, no recommendations were made on these two systemic weaknesses.

Processing Controls

Data processing controls ensured that DJMS-RC pay transactions were accurately computed for base pay, entitlements, and *   . However, without

---

*Sensitive computer security information deleted (DoD 5400.7-R).

improvements in the following processing controls, the integrity of pay data was not assured.

Consistency checking. Edits to ensure consistency of data were not performed. For example, unauthorized * payments and dual payments could be made to members. As a result, the * was incorrectly used during August 1996 in transactions involving 19 Army enlisted personnel. Yet, * is payable by regulation * . Likewise, consistency checking for * was not accomplished to prevent erroneous payments to members based on the member's * . Management was not aware of these system control weaknesses.

Generic COP. Use of the generic COPs was not adequately controlled or monitored. DJMS-RC programming requires that each transaction be identified by a COP code. With three exceptions, COP codes are unique and used to identify specific pay entitlements. However, three COPs were generic in nature and used for purposes not originally intended.

       o COP code "IS" identifies transactions subject to Federal Insurance Contribution Act and Federal and State income tax withholdings.

       o COP code "IT" identifies transactions subject to Federal and State income tax withholdings.

       o COP code "W7" identifies transactions exempt from tax withholding.

As a stopgap measure when the Army converted to DJMS in October 1992, Army requested that the three generic COPs be established for use through December 1993. These generic COPs were needed on a short-term basis because Army pay history data prior to October 1992 were not available to DJMS processing. Still used by Army, these COPs are now also used by Air Force to support entitlement payments:

       o for which there are no specific COPs assigned, such as to pay basic allowance for quarters adjusted for court ordered child support,

       o when the assigned COP does not accurately process (for example, to pay * for inactive-duty training), and

       o as a shortcut to simplify multiple or complicated transactions that typically cross several payment cycles.

---

*Sensitive computer security information deleted (DoD 5400.7-R).

The generic COPs are frequently used, as evidenced by the $533,000 in entitlement payments to Army and Air Force military members made during August 1996. When generic COPs are used, a member's retirement points are not calculated and credited toward future retirement. Also, the generic COPs do not identify the specific entitlement paid, and *

*

Each pay-affecting transaction for members on inactive-duty training or active-duty should be identified by a unique COP. Use of the generic COPs should be restricted to specific payments for limited time periods. Management agreed that the generic COPs were misused.

Audit Trails for Generic COPs. Without the addition of a memorandum entry, audit trails did not exist when the three generic COPs were used. Directives require a memorandum entry for each entitlement paid using these generic COPs. However, DJMS-RC does not systemically require a memorandum entry. The memorandum entry acts as the audit trail within DJMS-RC to explain the transaction, such as stating the entitlement being paid and inclusive dates of the payment. A review of 63 payments in August 1996 to Army and Air Force members identified 5 Air Force payments that did not have memorandum entries explaining the transaction. Without the memorandum entry, DJMS Denver could not identify the type of entitlement paid and had no assurance that the payment would not be duplicated in the future.

*   **Transactions.** *   transactions for active and inactive duty could bypass system edits.   Audit tests disclosed that DJMS-RC prematurely *   as paid to the *   before all processing was completed. However, subsequent processing might result in the payment being rejected. *

Bypassing this edit could result in duplicate payments.

Corrective Action. DJMS Denver was aware of the premature posting of transactions to the *   and prepared a system change to correct this systemic weakness. This request *   was approved by the change control board in May 1996. An implementation date has not been projected. Because of management's action, no recommendations have been made in this report. However, the DJMS Program Manager should ensure that the systemic changes required to correct this exposure are fully implemented.

---

*Sensitive computer security information deleted (DoD 5400.7-R).

Output Controls

Output controls over test transactions were adequate. Data inputs could be reconciled to output reports. Specifically, we input over 550 transactions to the DJMS Army and Air Force test systems. These test transactions included both correct and incorrect input data. The transactions were reported on the output reports as projected and were traced back to the original input transactions. The evaluation of output controls did not include a review of control totals or report distribution.

Conclusion

Management took corrective action to strengthen some DJMS-RC input and processing controls. However, additional system changes should be developed and implemented to:

> o include consistency checks for *

> o create unique components of pay for all current pay entitlements,

> o restrict the use of the generic components of pay, and

> o require a memorandum entry for all transactions using the generic components of pay.

Recommendations, Management Comments, and Audit Response

A. We recommend that the Program Manager, Defense Joint Military Pay System Program Management Office, Defense Finance and Accounting Service, implement functional system changes in the Defense Joint Military Pay System Reserve Component to:

> **1. Include consistency checks for *   .**

---

*Sensitive computer security information deleted (DoD 5400.7-R).

11

       2. Create unique components of pay for all current active-duty and inactive-duty-training pay entitlements.

       3. Restrict the use of the generic components of pay codes IS, IT, and W7 to specific payments for limited time periods.

       4. Systemically require a memorandum entry for all transactions using the generic components of pay.

Management Comments. DFAS concurred stating that a system change request to include consistency checks for *   will be prepared. In addition, unique components of pay will be created for all current training pay entitlements. The estimated completion dates for these system changes are August 31, 1997, and November 30, 1997, respectively.

A new Federal Managers' Financial Integrity Act, section 2, material weakness is being documented to identify use of the generic components of pay as a material weakness. This material weakness will be submitted to Headquarters, DFAS, by September 1, 1997. In addition, a system change will be implemented to provide the capability to monitor the use of "D" transactions for proper use of all components of pay. Estimated completion date for implementation of this change is September 30, 1997. DoD 7000.14-R, "DoD Management Regulation," Volume 7C, scheduled for January 15, 1998, publication will require the Reserve input source to monitor the use of generic components of pay and to establish procedures for reporting their continued misuse. In addition, Army, Air Force, and Navy managers will be tasked to change their Reserve Component input systems to require memorandum entries for all transactions using the generic components of pay. DJMS Denver will have followup responsibility until all changes are completed. The suspense date for this action is June 1998.

---

*Sensitive computer security information deleted (DoD 5400.7-R).

Finding B. Security Controls

The DMC-Denver and DJMS Denver can improve security for DJMS Army and Air Force.

    o The DJMS Air Force security structure did not give the DJMS Denver Information System Security Officers (ISSOs) proper administrative authority.

    o Access to sensitive command-level transactions for the individual DJMS production regions within the Customer Information and Control System (CICS) was not adequately controlled by DMC-Denver.

    o Personnel with sensitive system access assigned to the Software Engineering Directorate did not have required background investigations.

The DJMS Air Force security environment established by DMC-Denver did not give the DJMS Denver ISSOs adequate authority to administer security over Air Force military pay data and DJMS core resources. DMC-Denver had not performed a review of the CICS command-level transactions for either the DJMS Army or Air Force production regions. Software Engineering Directorate management had not adequately evaluated sensitive system access permissions granted to their personnel. Inadequate security administration allowed knowledgeable users to manipulate DJMS resources without detection. As a result, the integrity of DJMS Army and Air Force data was not safeguarded.   The inadequate controls over DJMS constituted a material management control weakness.

Security Environment

Security Software. For DJMS and other applications identified to and protected by CA-Top Secret security software at DMC-Denver, security is structured within defined layers: central, zone, division, and department. A security administrator generally has authority over application resources and users that fall under his or her functional area of administration. Security within these layers can only be administered down to the next defined layer. Thus, security cannot be administered from a lower layer up or across to another security layer. As illustrated in Figure 1, a department defined by CA-Top Secret cannot administer security over a division. Likewise, one department cannot have security authority over another department even within the same zone.

DoD Directive. DoD Directive 5200.28, "Security Responsibilities for Automated Information Systems (AISs)," March 21, 1988, directs the head of

13

each DoD Component to assign an official as the Designated Approving Authority (DAA) responsible for ensuring compliance with AIS security requirements. The DAA is to ensure that an ISSO is named for each AIS. The directive gives the ISSO security responsibility and authority for the AIS. Specifically, each ISSO shall:

> Ensure that the AIS is operated, used, maintained, and disposed of in accordance with internal security policies and practices. . . . Have the authority to enforce security policies and safeguards on all personnel having access to the AIS for which the ISSO has cognizance.

DJMS was identified as a Headquarters, DFAS, automated information system. The DAA for the DJMS application was the Deputy Director of the Information Management Deputate. The ISSOs assigned to DJMS Denver were responsible for securing DJMS Air Force and all DJMS core resources.

DFAS Implementation.   In implementing the DoD directive, the DFAS 8000.1-R, "Information Management Policy and Instructional Guidance," Version 4, August 21, 1996, created an Information Security Officer (ISO) between the DAA and ISSO. The ISO for DJMS is at Headquarters, DFAS. The DFAS Denver Center ISO did not have security responsibility for DJMS. However, as detailed below, DMC-Denver planned to assign zone security responsibilities over the DJMS and other applications to the DFAS Denver Center ISO.

DJMS Air Force Security

The security structure defined by DMC-Denver placed DJMS Air Force as 1 of 14 divisions to be administered by the DFAS Denver Center ISO.   This structure did not permit the DJMS Denver ISSOs proper administrative authority over the application processing environment and DJMS core resources.   In coordination with DJMS Denver and other customers, the DMC-Denver is responsible for establishing the security structure for the applications on their mainframes.   That responsibility includes acting as the CA-Top Secret central security administrator for the applications.   Figure 1 illustrates the current security structure that was implemented by DMC-Denver without coordinating with DJMS Denver.
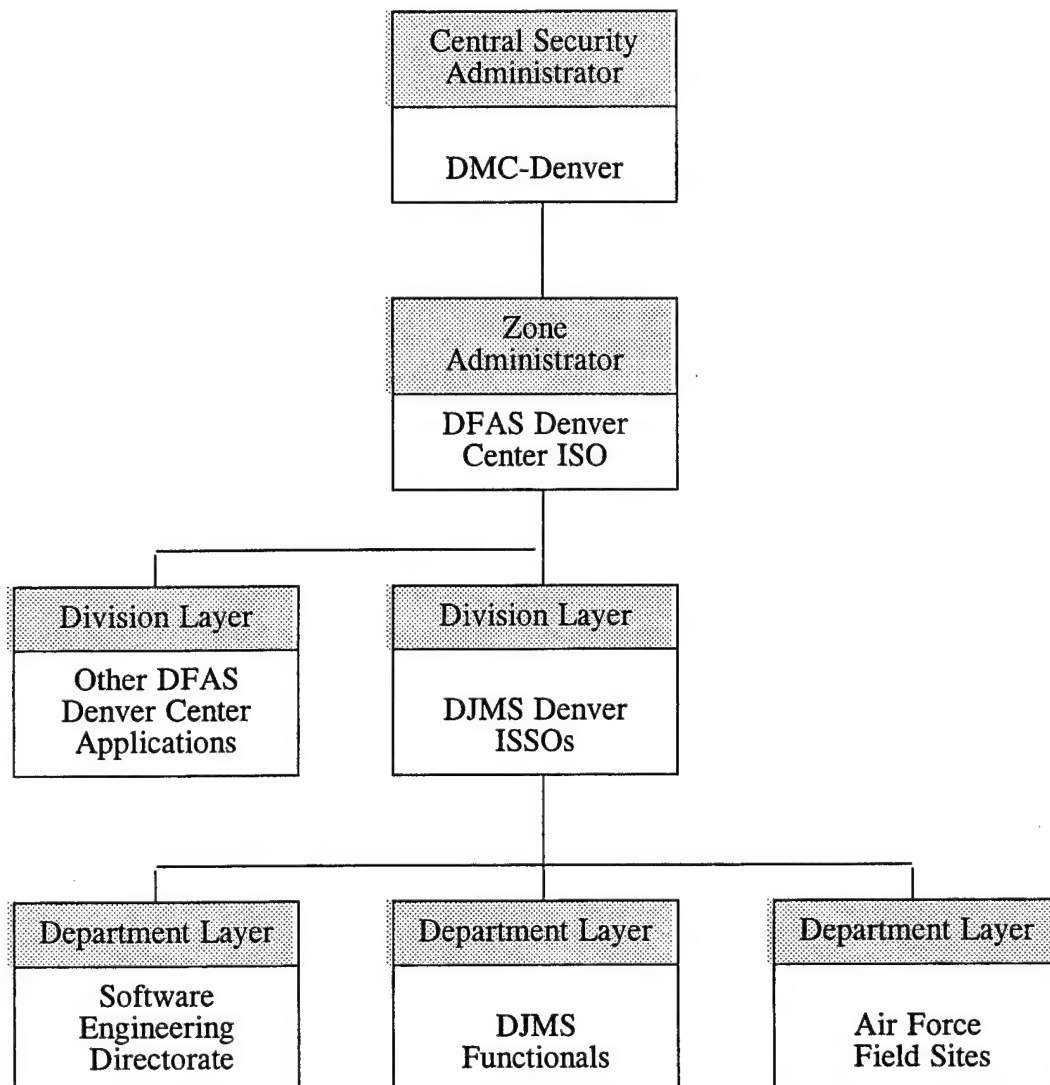
Figure 1. Security Structure Supporting the Defense Joint Military Pay System for Air Force

Effect on Application Security. The current security structure implemented by DMC-Denver for DJMS Air Force does not provide adequate security administrative authority to the DJMS Denver ISSOs who are responsible for securing the application resources. First, the DMC-Denver intended to establish the DFAS Denver Center ISO as zone administrator over DJMS Air Force resources. Thus, DMC-Denver created the framework to allow user access to DJMS resources without the knowledge or authorization of the DJMS Denver ISSOs. As a result, the integrity of DJMS Air Force military pay data was not ensured.

Second, without the knowledge or approval of DJMS Denver, the DMC-Denver created an additional security division for the exclusive use of the Software Engineering Directorate, which is dedicated to DJMS support. This action was taken in response to an October 22, 1996, memorandum from the Software Engineering Directorate requesting that:

    o four high-level DJMS datasets[4] be created for their dedicated use for DJMS job runs, and

    o security for the new datasets be handled only by the DMC-Denver security office.

The request explicitly stated that the DJMS Denver ISSOs were not to have access to these new datasets, thus purposely circumventing the authority and control of the DJMS Denver ISSOs.

The placement of this new division within that security structure is illustrated at Figure 2. Although not apparent from the figure, four newly created high-level datasets and four profiles were identified to this division. Each profile had a collection of access characteristics common to several users within the Software Engineering Directorate. Although the DMC-Denver knew the Software Engineering Directorate was dedicated to DJMS support, the Megacenter still created the new division, datasets, and profiles without the knowledge or approval of DJMS Denver. Because this new division was at the same security level as the DJMS Denver division, the DJMS Denver ISSOs could not administer security over this new division. Thus, by circumventing the authority and responsibility of the DJMS Denver ISSOs, DJMS Air Force and core resources were exposed to unnecessary risk.

---

[4]A dataset is a collection of related computer bytes, such as a file of payroll records or a library of payroll programs.
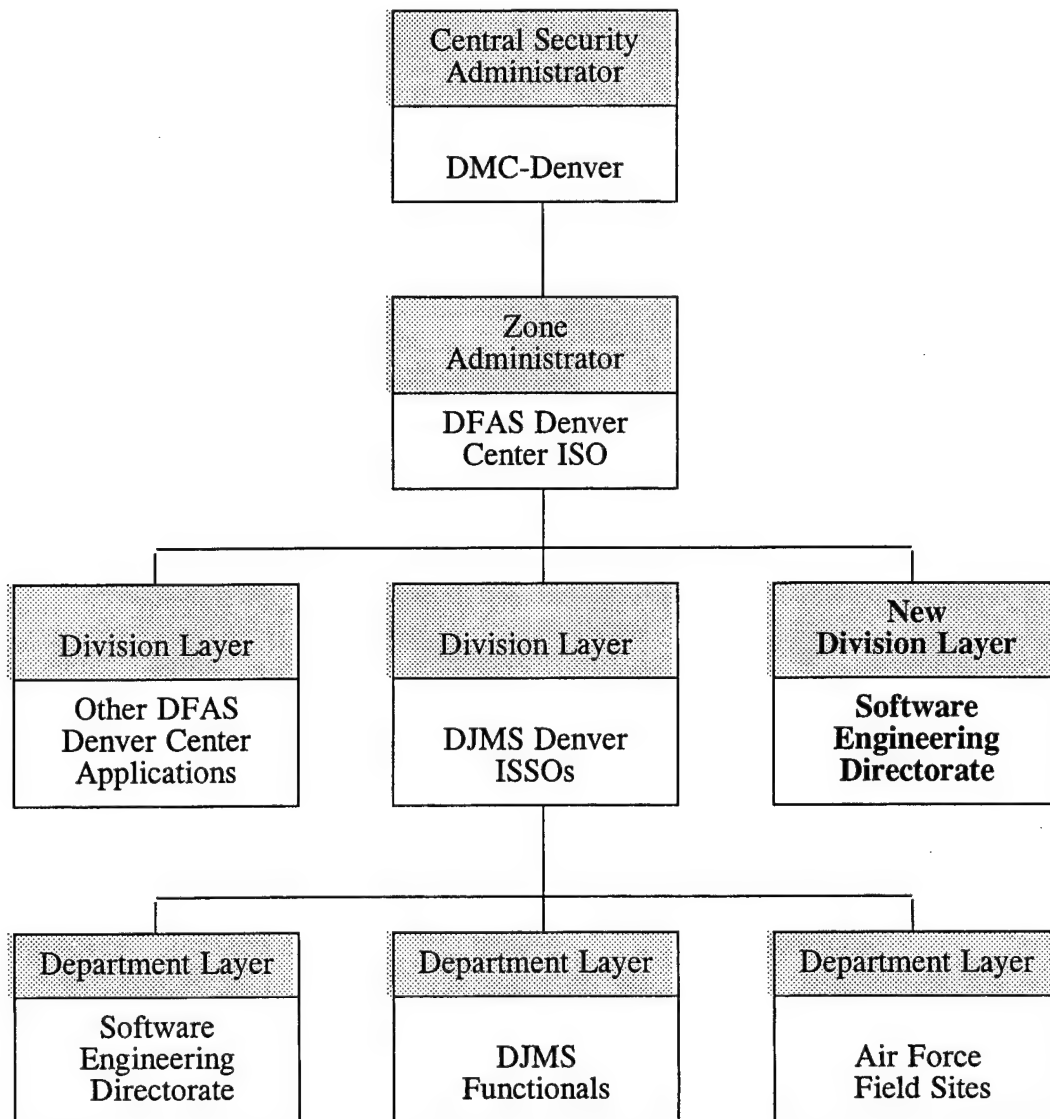
Figure 2.   Changed Security Structure Supporting the Defense Joint Military Pay System for Air Force

Repeat Finding.   A similar finding was reported in Inspector General (IG), DoD, Report No. 96-175, "Computer Security Over the Defense Joint Military Pay System," June 25, 1996.   The report stated that DMC-Denver created new divisions and departments with access to DJMS Army resources

17

without the knowledge or approval of DFAS Indianapolis. As identified in that report and again in this finding, DMC-Denver permitted access to application resources without the approval of the appropriate security administrator.

Corrective Actions. To execute their security responsibilities under DoD Directive 5200.28, DJMS Denver ISSOs should have CA-Top Secret authority to effectively administer security over the DJMS Air Force and all DJMS core resources. To accomplish this without compromising security for other DFAS Denver Center applications, DJMS Air Force should be placed within a zone dedicated solely to securing the resources of that application. Figure 3 illustrates one possible security environment for DJMS Air Force. This environment should be established at the discretion of the DMC-Denver and in full agreement with DJMS Denver.

In a December 13, 1996, memorandum to the Director, DMC-Denver, the Director of DJMS Denver requested that the DJMS Denver ISSOs be reinstated as zone administrators to effectively perform security tasking over their application. DJMS Denver also stated that all requests for access to DJMS resources were to be submitted through the DJMS Denver security office. In response to audit concerns and requests by the Software Engineering Directorate and DJMS Denver, DMC-Denver deleted the new security division created for the Software Engineering Directorate as well as the datasets and profiles. In addition, DMC-Denver agreed with our assessment to redefine the DJMS security structure. In February 1997, the DMC-Denver placed DJMS in a CA-Top Secret security zone dedicated to the application. As a result of management's action, no recommendation was made in this report to redefine the existing security structure for DJMS. However, security administrative authority over this zone and the resources identified to it had not been and must still be defined.

Further, in response to a recommendation in Report No. 96-175, DFAS is developing a memorandum of agreement that states the authority and responsibility for defining, controlling, and monitoring user access to DJMS. Although this document had not been finalized, DFAS believed the agreement will resolve the issues concerning security changes that affect DJMS and granting access to DJMS resources.
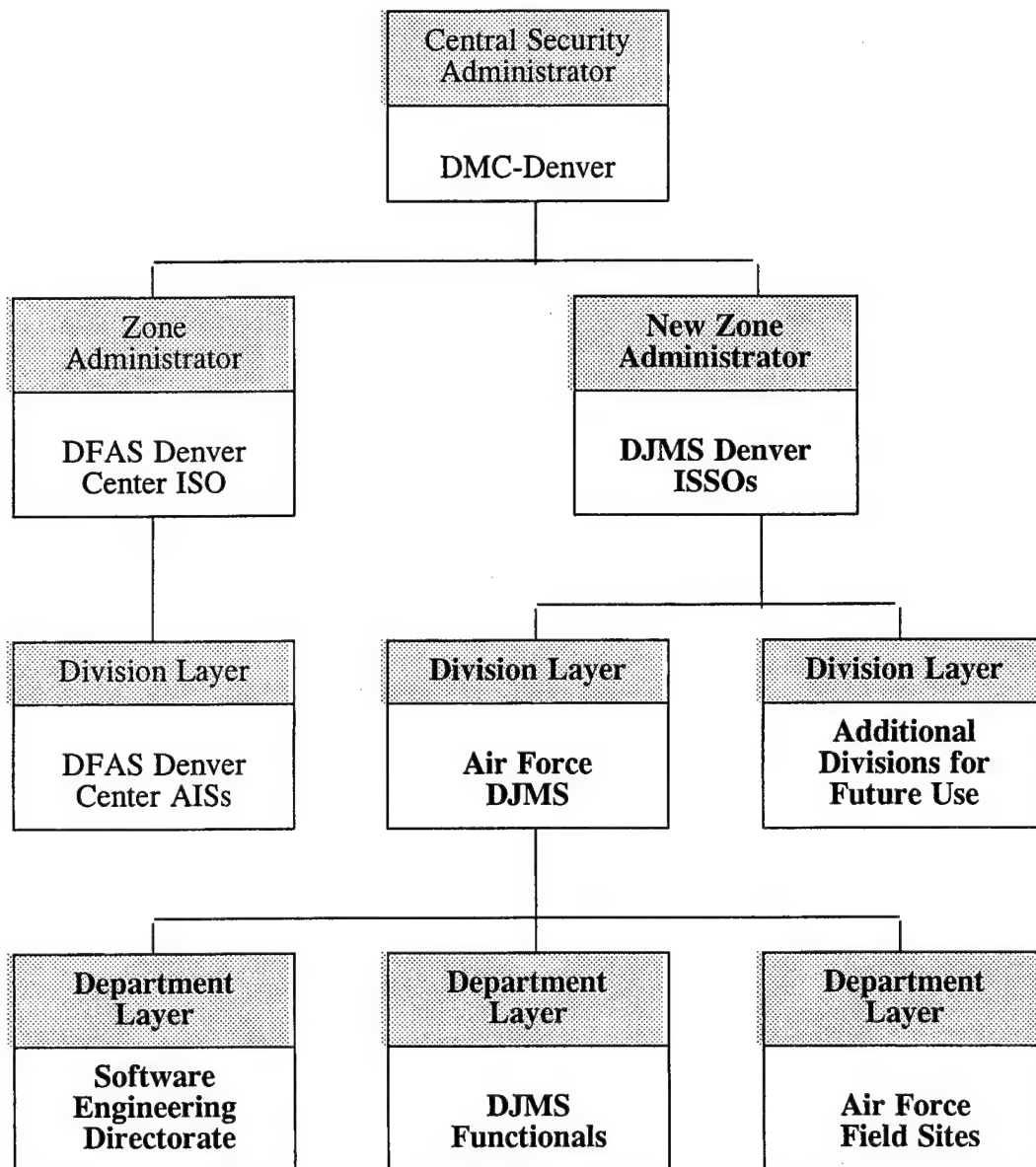
Figure 3. Suggested Security Structure Supporting the Defense Joint Military Pay System for Air Force

Command-Level Transactions for the Customer Information and Control System

CICS Regions. Both DJMS Army and Air Force are identified to CICS regions dedicated solely to their production processing. CICS acts as the interface between the mainframe and the application and permits concurrent

19

processing of transactions entered from different terminals. It provides the functions and facilities essential to the creation, operation, and maintenance of an on-line system. Security and control of a CICS region and the integrity of data defined to the region are controlled by command-level transactions, such as the Master Terminal Operator command. Only a limited number of personnel should be able to execute these commands because of their high-level capabilities.

Command-Level Controls. Access to CICS command-level transactions was not adequately restricted for the separate DJMS Army and Air Force production regions. Although DMC-Denver is responsible for controlling and maintaining these CICS regions, it had not performed a review of the command-level controls. As a result, the command-level transactions were not adequately restricted to personnel with a need to know. For example:

    o 33 individual users in the Software Engineering Directorate and 12 DMC-Denver users were granted access to the Master Terminal Operator command within the DJMS Air Force production CICS region.

    o 46 individual users in the Software Engineering Directorate and 81 DMC-Denver users were granted the same access within the DJMS Army production region.

The Master Terminal Operator command allows authorized users to perform sensitive tasks such as terminating ongoing jobs, shutting down CICS, and altering processing priority. DMC-Denver agreed that access to these CICS transactions was excessive and should be reviewed. Because access to the command-level transactions is granted to individual users in addition to DJMS profiles, the review should be coordinated with DJMS Indianapolis, DJMS Denver, and the Software Engineering Directorate.

Critical-Sensitive Ratings

Inadequate security controls existed over individuals with sensitive access to DJMS software and pay data. Similar problems were identified in prior and ongoing audits at other DFAS organizations, indicating a pattern of noncompliance within DFAS.

    o Positions were not properly designated critical-sensitive or required background investigations had not been completed, as required by DoD 5200.2-R, "Personnel Security Program," January 1987.

    o ISSOs did not adequately enforce the security requirements of DoD Directive 5200.28. The ISSOs granted sensitive access to DFAS computer resources without verifying that the requirements of DoD 5200.2-R were met.

Security Requirements. DoD 5200.2-R requires the following actions:

o Classify positions as critical-sensitive if they give individuals access to computer systems that could be used to cause grave damage to the application or data during its operation or maintenance.

o Before their appointment, complete background investigations on employees who will occupy critical-sensitive positions.

o Obtain a waiver from the designated official if the delay in appointing someone to a critical-sensitive position without a completed background investigation would be harmful to national security.

In fulfilling their security oversight role under DoD Directive 5200.28, ISSOs should verify that these requirements have been met before granting access to sensitive computer resources of DJMS or other applications. Before granting access to an AIS, DFAS security personnel are required by DFAS 8000.1-R to verify that users have a need to know and have undergone the prescribed background investigation, commensurate with the designated position sensitivity.

Repeat Finding. As detailed in Appendix B, our first DJMS audit (Report No. 96-175) determined that the Software Engineering Directorate had not properly classified critical-sensitive positions, requested required background investigations, or obtained necessary interim waivers. In response to recommendations made in the report, the Director, DFAS Financial Services Organization, stated in April 1996 that:

o sensitive positions pertaining to DJMS had been reviewed,

o required waivers had been signed for personnel assigned to these positions,

o all directors had been informed of required procedures regarding sensitive positions, and

o periodic surveys of the organization's posture regarding sensitive positions had been mandated.

Despite these directions, the current audit determined that 19 personnel and 1 contractor assigned to the Software Engineering Directorate in Denver and 4 personnel in Indianapolis still did not have background investigations or interim waivers. Although some corrective actions were taken, the audit showed that a thorough review of all users with sensitive access was not accomplished.

Security Oversight. In granting sensitive access to Software Engineering Directorate users, the DJMS Denver ISSOs did not enforce the security requirements of DoD Directive 5200.28 or DFAS 8000.1-R. DJMS Denver ISSOs should verify that users requesting access to sensitive DJMS resources have background investigations or required interim waivers.

DFAS Compliance. Noncompliance with DoD 5200.2-R is a continuing problem within DFAS, not limited to the Software Engineering Directorate.

o An ongoing audit of the DFAS Enterprise local area network determined that sensitive positions were not properly classified as critical-sensitive. As a result, background investigations and required interim waivers had not been obtained for personnel assigned to these positions.

o Likewise, an ongoing audit of the DFAS Defense retiree and annuitant system also determined that sensitive positions were not properly classified as critical-sensitive. Consequently, required background investigations and interim waivers had not been obtained. In some instances, background investigations had not been properly updated.

Though not addressed in prior reports, the ISSOs at these other DFAS organizations obviously did not fulfill their security oversight roles under DoD Directive 5200.28. Otherwise, these ISSOs would not have granted access to sensitive computer resources. This problem continues; the DFAS network audit determined that network ISSOs granted access to sensitive resources without verifying that all users had required background investigations or interim waivers.

Personal Integrity of Employees. Meeting the requirements of DoD 5200.2-R is important to maintaining security for DJMS and other DFAS applications. Personnel in critical-sensitive positions have a high-level of access to DFAS computer resources and, therefore, are not easily subject to management oversight and control. The personal integrity of such employees is an important control. Without the critical-sensitive designation and related background investigation, management has less assurance that personnel placed in positions with critical access capability are worthy of public trust.

Corrective Actions. When notified of these conditions, the Software Engineering Directorate took immediate corrective action to remove sensitive access from one individual. In addition, interim waivers were completed for 4 personnel and 13 additional positions were identified for critical-sensitive ratings based on current system access capabilities. Background investigations were still required for the 13 personnel assigned to these positions. Interim waivers should be provided until the background investigations are completed.

DFAS managers at different organizational levels have attempted to comply with the DoD requirements. However, despite such attempts, noncompliance continues to occur. Direction and oversight by Headquarters, DFAS, is required if this problem is to be resolved.

Conclusion

Management took some corrective actions to strengthen security for the DJMS Army and Air Force. However, the following additional measures should be taken:

o Provide the DJMS Denver ISSOs proper security administrative authority over DJMS Air Force and core resources.

o Control access to sensitive command-level transactions for the DJMS Army and Air Force production CICS regions.

o Acquire required background investigations for personnel with sensitive DJMS access.

Recommendations, Management Comments, and Audit Response

B.1. We recommend that the Director, Defense Megacenter, Denver, Colorado, Defense Information Systems Agency:

a. Provide advance written notification of all security changes directly or indirectly affecting the Defense Joint Military Pay System to the Information System Security Officers, Directorate of Military Pay, Defense Finance and Accounting Service Denver Center, Denver, Colorado.

b. Receive approval from the Information System Security Officers, Directorate of Military Pay, Defense Finance and Accounting Service Denver Center, Denver, Colorado, before granting access to any Air Force Defense Joint Military Pay System resource.

c. Review the Customer Information and Control System command-level transactions for the individual Defense Joint Military Pay System production regions and limit access to these transactions to individuals with a need to know.

Management Comments. DISA concurred with all recommendations. The DMC-Denver will provide written notification to the Information System Security Officers, Directorate of Military Pay, DFAS Denver Center, of all security changes that affect DJMS. In addition, these security officers will approve access to all Air Force DJMS resources. The DMC-Denver incorporated these recommendations into its procedures as of May 1, 1997. Accordingly, management completed action on both recommendations.

DMC-Denver completed a review of sensitive CICS Owned Transactions. Further review is required to determine whether the access levels are necessary

and appropriate. The DMC-Denver also identified additional sensitive CICS transactions for review. This review and any necessary updates will be completed by July 31, 1997.

B.2. We recommend that the Director, Directorate of Software Engineering-Military Pay, Defense Finance and Accounting Service, request access to all Defense Joint Military Pay System resources directly from the Information System Security Officers, Directorate of Military Pay, Defense Finance and Accounting Service Denver Center, Denver, Colorado.

Management Comments. DFAS concurred with this recommendation. Procedures have been established to request system access authorization through the DJMS coordinating Information System Security Officer.

B.3. We recommend that the Director, Defense Finance and Accounting Service, emphasize the importance of security directives by requiring each center director and the Deputy Director, Information Management Deputate, to provide written assurance that:

a. The sensitivity level assigned to all personnel positions is in accordance with DoD 5200.2-R, "Personnel Security Program," January 1987.

b. All personnel with sensitive access to automated information systems have background investigations (and where appropriate, interim waivers pending completion of such investigations), as required by DoD 5200.2-R.

Management Comments. DFAS partially concurred with the recommendations. DFAS recognized the need to aggressively emphasize the importance of security issues but disagreed with the need to send a formal memorandum to the Director, DFAS, as recommended. DFAS 8000.1-R, "Information Security Policy," is being revised to address sensitive positions in accordance with DoD 5200.2-R. The scheduled publication date for the revised DFAS regulation is July 30, 1997. Use of current DFAS forms accommodate sensitivity designations commensurate with position duties and ensure that the appropriate background investigation is either on record or has been initiated.

Audit Response. We consider the DFAS comments to Recommendations B.3.a. and B.3.b. to be nonresponsive. Although revising DFAS 8000.1-R is a positive step toward making management more aware of the sensitive position designation requirements, it will not ensure that the criteria of DoD 5200.2-R are met. The requirements of this Regulation have existed since January 1987. They have been brought to the attention of DFAS managers on prior audits, yet noncompliance with the Regulation continues. Likewise, use of the DFAS Forms 113 and 114 are purported to accommodate sensitivity designations commensurate with position duties. These forms have been in use since 1993,

24

yet they have not guaranteed that sensitive positions were appropriately rated or background investigations performed on individuals with sensitive system access. As a result, we believe it is imperative that these requirements be monitored by the Director, DFAS, to ensure that the criteria of DoD 5200.2-R are met. We request that DFAS reconsider its position and provide additional comments on Recommendations B.3.a and B.3.b.

This page was left out of orignial document

26

Part II - Additional Information

27

Appendix A. Audit Process

Scope and Methodology

Audit Methodology. We examined application controls for DJMS-RC production processing. In addition, we evaluated security software controls over the DJMS Army and Air Force active-duty and Reserve components. Specifically, we evaluated:

     o application controls over data input, processing, and output in DJMS-RC production processing,

     o the security environments for DJMS Army and Air Force production processing, including controls over selected CICS command-level transactions, and

     o controls over DJMS resources, including those limiting access to authorized users.

To evaluate application controls, we used the separate mainframe test environments established for DJMS Army and Air Force. These test environments duplicate DJMS production processing. Fictitious military pay accounts were established and transactions submitted to test controls over five pay entitlements *

                                               and three
generic COPs (IS, IT, and W7). The Reserve Component Input Sub-System, a microcomputer-based data-entry system, was used to create all test transactions. This system is used by multiple Army and select Air Force sites for data entry into DJMS-RC. To provide impact to the identified processing vulnerabilities, entitlement data in the MMPA records and the August 1996 voucher payment files were extracted for manual review. Only abnormal or unusual payments were tested against regulatory criteria. Examples of these results were then quantified and reported under Finding A. Because tests were performed on a limited basis, additional exceptions may exist beyond those identified in this audit.

To test security rules and features and access authorizations, we used the audit features of the CA-Top Secret security software. The results of these tests were reported under Finding B. We also used the CA CULPRIT report writer to extract pay transaction data directly from the DJMS MMPA records and the August 1996 voucher files of Army and Air Force payments.

---

*Sensitive computer security information deleted (DoD 5400.7-R).

Audit Scope. Because of the size and complexity of DJMS, we limited our review to application and security controls over the DJMS Reserve Component, as discussed above. Likewise, the evaluation of output controls did not include a review of control totals or report distribution.

Use of Statistical Sampling Procedures and Computer-Processed Data. We did not rely on statistical sampling procedures to achieve the audit objectives. However, we did rely on computer-processed data extracted from the security software database provided by CA-Top Secret, the August 1996 voucher files of Army and Air Force payments, and the MMPA records for Army and Air Force members. All system testing and use of security software audit tools were accomplished in a controlled environment with management's approval. We used automated and manual techniques to analyze system data. Based on those tests and assessments, we concluded that the data were sufficiently reliable to be used in meeting the audit objectives.

Audit Type, Dates, and Standards. This financial-related audit was performed from March 1996 through April 1997. The audit was made in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the IG, DoD, and accordingly included such tests of management controls as were considered necessary.

Contacts During the Audit. We visited or contacted individuals and organizations within the DoD. Further details are available on request.

Management Control Program

DoD Directive 5010.38, "Internal Management Control Program," April 14, 1987,[1] requires DoD organizations to implement a comprehensive system of management controls that provides reasonable assurance that programs are operating as intended and to evaluate the adequacy of the controls.

Scope of Review of Management Control Program. We reviewed the implementation of the DoD management control program at the DFAS Indianapolis and Denver Centers and at the DMC-Denver. Specifically, we evaluated the adequacy of management controls over the processing of payments by and security of DJMS-RC. We also reviewed the results of the management's self-evaluation of those controls.

---

[1]DoD Directive 5010.38 has been revised as "Management Control Program," August 26, 1996. The audit was performed under the April 1987 version of the directive.

Adequacy of Management Controls. We identified material management control weaknesses at the DFAS level, as defined by DoD Directive 5010.38, in the process used by the DJMS Denver to pay military reserve and national guard members. Improvements were needed in the management controls over pay entitlements, *   , use of and audit trails for generic components of pay, *   transactions,   unreasonable *   ,   premature *   , and user access. The integrity of and security over the DJMS military pay data will be improved by implementing:

     o The three system changes *   identified in Finding A, and

     o Recommendations A.1. through A.4., B.2., B.3.a., and B.3.b.

A copy of the report will be provided to the senior DFAS official responsible for internal controls. We also identified material management control weaknesses at the DMC-Denver level, as defined by DoD Directive 5010.38, in the procedures used by the megacenter to secure computer data. Management controls over granting access to DJMS files and CICS transactions needed improvement. Implementing Recommendations B.1.a. through B.1.c. should improve the security over DJMS military pay data.

Adequacy of Management's Self-Evaluation. Officials at DFAS Denver Center identified the operations in DJMS-RC as a part of the Reserve Component System Division. They had performed a risk assessment and correctly assigned a high risk to this area. Management performed an internal management control review of the unit in 1995. Management did not report the material weaknesses identified in the audit because they reported them in the annual report on the DFAS Denver Center operating accounting systems (formerly the Federal Manager's Financial Integrity Act Section 4 report). However, the Director, DFAS Denver Center, requested the current and prior DJMS audits, which reviewed DJMS management controls. Officials at the DFAS Indianapolis Center identified the Reserve pay system as part of the Reserve Component Systems Office. They had performed a risk analysis and correctly assigned a medium risk because this unit does not include any DJMS-RC core processing. Further testing was not accomplished.

The DMC-Denver officials identified their security operations as part of the DMC-Denver assessable unit. However, DMC-Denver assigned a low risk to that assessable unit and had not performed a test of the applicable management controls. We believe that DMC-Denver should have assigned a high level of risk to the area and should have conducted an evaluation of the applicable management controls. Because DMC-Denver did not conduct an evaluation, they did not identify or report the material management control weaknesses identified in the audit.

---

*Sensitive computer security information deleted (DoD 5400.7-R).

Appendix B. Summary of Prior Coverage

During the past 5 years, the IG, DoD, and the Army Audit Agency issued five reports related to DJMS-RC application controls and security. The two problems discussed in Part I, Finding B, concerning the creation of new CA-Top Secret security areas and the absence of required background investigations were also addressed in IG, DoD, Report No. 96-175. These two problems are repeat findings. The reports issued on these prior audits are discussed below.

Inspector General, DoD

Report No. 96-175, "Computer Security Over the Defense Joint Military Pay System," June 25, 1996. The audit focused on access to the active-duty DJMS component but reviewed some elements of DJMS-RC security administration. The report states that the DMC-Denver permitted access to DJMS Army resources without the approval of DFAS Indianapolis. Because of other circumstances that existed at the time of the audit, a specific recommendation was not directed to the Megacenter.

In addition, sensitive system positions for 41 programmers assigned to the Software Engineering Directorate were not properly designated critical-sensitive as required by DoD 5200.2-R. In addition, pending completion of required background investigations, interim waivers were not obtained for 28 personnel assigned to critical-sensitive positions within the Software Engineering Directorate at Denver. The Director, DFAS Financial Systems Organization, concurred with the recommendations to designate all sensitive positions in the Software Engineering Directorate as critical-sensitive and obtain background investigations (or interim waivers) on all personnel in critical-sensitive positions and before appointing new personnel to such positions. Management stated that all positions had been reviewed and waivers signed before the audit was completed. However, the current audit determined that all personnel with critical access still did not have background investigations or interim waivers, as explained in Finding B.

Report No. 94-065, "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service," March 24, 1994. The audit evaluated management controls over selected features of the operating system and security software used to safeguard the integrity of DFAS data at four DoD locations. The report identified 13 sensitive system positions that had not been designated critical-sensitive at the DFAS Financial Systems Activity in Pensacola, Florida. Management concurred with the audit recommendations to designate those positions as critical-sensitive and obtain the necessary background investigations. Subsequent audit followup verified that management had initiated corrective action.

Army Audit Agency

Report No. 95-737, "Audit of Selected Army Reserve Pay Issues," July 7, 1995. The audit determined that the Army Reserve had adequate controls over incentive payments but that some personnel received duplicate bonus payments. The duplicate payments occurred because DJMS-RC did not have adequate software edits to prevent these transactions from processing. Management concurred with the recommendation to identify and collect duplicate bonus payments and to establish a control mechanism to preclude additional duplicate payments from occurring until the software problem is corrected.

Report No. 95-722, "Controls Over Reserve Component Pay," April 21, 1995. This report focused on input and management controls of pay units at the field level. The report did not involve any review of the DJMS mainframe system controls; however, one issue related to our audit objective was discussed. The report states that pay clerks had unrestricted access to DJMS-RC pay files and could change information in pay records that affected the pay computation. The audit reviewed the management controls at the bases and did not find any instances where payroll clerks made unauthorized changes to pay files. Recommendations were not made because management was taking action to correct the weakness.

Report No. 95-725, "Audit of Selected National Guard Pay Issues," April 14, 1995. The audit reviewed manual controls initiated by the Army National Guard to avoid duplicate processing of bonus payments. These controls were necessary because the DJMS-RC did not contain software edits to prevent processing duplicate bonus payments. The Army Audit Agency made no recommendations because the National Guard took corrective actions before the end of the audit.

Appendix C. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense (Comptroller)
   Deputy Chief Financial Officer
   Deputy Comptroller (Program/Budget)
Director, Administration and Management (Internal Control Officer)
Director, Defense Logistics Studies Information Exchange

Department of the Army

Chief, National Guard Bureau
Auditor General, Department of the Army

Department of the Navy

Assistant Secretary of the Navy (Financial Management and Comptroller)
Auditor General, Department of the Navy

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Auditor General, Department of the Air Force

Other Defense Organizations

Director, Defense Contract Audit Agency
Director, Defense Finance and Accounting Service
   Internal Control Office, Audit Control Office, Office of the Director
Director, Defense Information Systems Agency
   Inspector General, Defense Information Systems Agency
   Internal Control Officer, Defense Information Systems Agency, Office of the
      Comptroller
Director, Defense Logistics Agency
Director, National Security Agency
   Inspector General, National Security Agency
Inspector General, Defense Intelligence Agency

Non-Defense Federal Organizations and Individuals

Special Projects Branch, National Security Division, Office of Management and Budget
Technical Information Center, National Security and International Affairs Division,
    General Accounting Office

Chairman and ranking minority member of each of the following congressional
    committees and subcommittees:

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on National Security, Committee on Appropriations
House Committee on Government Reform and Oversight
House Committee on Government Management, Information, and Technology,
    Committee on Government Reform and Oversight
House Subcommittee on National Security, International Affairs, and Criminal
    Justice, Committee on Government Reform and Oversight
House Committee on National Security

Part III - Management Comments

Defense Finance and Accounting Service Comments

DEFENSE FINANCE AND ACCOUNTING SERVICE
1931 JEFFERSON DAVIS HIGHWAY
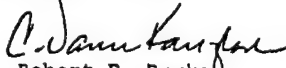ARLINGTON, VA 22240-5291

JUN 30 1997

DFAS-HQ/S

MEMORANDUM FOR ACTING DIRECTOR, FINANCE AND ACCOUNTING
DIRECTORATE, DEPARTMENT OF DEFENSE,
INSPECTOR GENERAL

SUBJECT: Audit Report on Application Controls Over the
Defense Joint Military Pay System Reserve
Component (Project No. 6FD-2015)

We have reviewed the subject audit report. We concur
with the recommendations for findings A.1, A.2, A.3, A.4,
and B.2; however, we partially concur with B.3, as shown in
the attachment.

My point of contact for this audit is Ms. Ethel
Matthews, DFAS-HQ/SC, (703) 607-3972, DSN 327.

for Robert E. Burke
Deputy Director for
Information Management

Attachment
as stated

cc: DFAS-HQ/PA
DFAS-HQ/FMM
DJMS Program Manager
DFAS-HQ/H
DFAS-DE/FJ
DFAS-DE/DIB
FSA-DE

FINAL AUDIT REPORT
OF
APPLICATION CONTROLS OVER THE
DEFENSE JOINT MILITARY PAY SYSTEM RESERVE COMPONENT
PROJECT NUMBER 6FD-2015

Finding A: Data Input, Processing and Output Controls

Recommendation A.1: Include consistency checks for
*
      .

DFAS Comments: CONCUR. The Denver Center, Directorate of
Military Pay, Reserve Component Systems Division, will
prepare a system change request (SCR) to include
consistency checks for *
          . The estimated completion date for implementing
this SCR is August 31, 1997.

Recommendation A.2: Create unique components of pay for
all current active-duty and inactive-duty training pay
entitlements.

DFAS Comments: CONCUR.

As a part of the overall migration effort, a component of
pay scrub is presently being accomplished by the Reserve
Component Systems Division. Unique components of pay
(COPs) will be created for all current active-duty and
inactive-duty training pay entitlements as a result of the
COP scrub. The scrub is expected to be completed by
August 30, 1997. The COP scrub will include a line item
by line item revalidation of each item on the COP table.
The estimated completion date for implementing the
resulting SCR(s) is November 30, 1997.

Recommendation A.3: Restrict the use of the generic
components of pay codes IS, IT, and W7 to specific
payments for limited time periods.

DFAS Comments: CONCUR.

(1) A new Federal Manager Financial Integrity Act Section
2, material weakness is being documented to address this
recommendation. The estimated completion date for

*Sensitive computer security information deleted (DoD 5400.7-R).

submission of the material weakness to DFAS-HQ is
September 1, 1997.

(2)   The Reserve Component System Division will prepare an
SCR to build the capability to monitor the use of "D"
transaction identification number (TINs) for proper
components of pay that will also include use of generic
components of pay IS, IT, and W7.   The estimated
completion date for implementing this SCR is September 30,
1997.

(3)   The reserve input source will be responsible for
monitoring the use of the generic COPs and establishing
standards for how often the COPs will be monitored as well
as procedures for reporting continued misuse of the
generic COPs.   This requirement will be included in the
DoD Financial Management Regulation Vol. 7C which is
scheduled for publication by January 15, 1998.

Recommendation A.4: Systematically require a memorandum
entry for all transactions using the generic components of
pay.

DFAS Comments: CONCUR.   The Reserve Component Systems
Division, DFAS-DE/FJR, will release a letter by July 31,
1997, tasking all Army, Air Force and Navy managers of
Reserve Component input systems requesting them to change
their input systems, with a suspense date of June 1998.
DFAS-DE/FJR will have follow-up responsibility for this
action until all changes are completed.

Finding B: Security Controls

Recommendation B.2:   We recommend that the Directorate of
Software Engineering-Military Pay, Financial Systems
Activity, request access to all Defense Joint Military Pay
System resources directly from the Information System
Security Officers, Directorate of Military Pay, Defense
Finance and Accounting Service Denver Center, Denver,
Colorado

DFAS Comments: CONCUR.   Specific procedures have been
established internally to request systems access
authorization through the DJMS coordinating Information
System Security Officer.

Recommendation B.3:   We recommend that the Director,
Defense Finance and Accounting Service, emphasize the
importance of security directives by requiring each Center

Director and the Deputy Director, Information Management
Deputate, to provide him written assurance that:

Recommendation B.3.a: The sensitivity level assigned to
all personnel positions is in accordance with DoD 5200.2-
R, "Personnel Security Program," January 1987.

Recommendation B.3.b: All personnel with sensitive access
to automated information systems have background
investigations (and where appropriate, interim waivers
pending completion of such investigation), as required by
DoD 5200.2-R.

DFAS Comments: PARTIALLY CONCUR. We concur with the need
to aggressively continue to work this issue, although we
disagree with the need for each Center Director to send a
formal memorandum to the Director, Defense Finance and
Accounting Service, as recommended. The DFAS 8000.1-R,
"Information Security Policy," is being revised to address
sensitive positions in accordance with DoD 5200.2-R,
"Personnel Security Program." The revised publication
will be published by July 30, 1997. Use of the DFAS 113
"Position Designation Record" and DFAS Form 114 "Pre-
Appointment Investigate Requirement Check," accommodate
sensivity designation commensurate with position duties,
as well as ensure the appropriate background investigation
is either on record or initiated with a waiver.

Defense Information Systems Agency Comments

DEFENSE INFORMATION SYSTEMS AGENCY
701 S. COURTHOUSE ROAD
ARLINGTON, VIRGINIA 22204-2199

IN REPLY
REFER TO: Inspector General   10 June 1997

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE
           ATTN: Financial Services Division (Denver),
              Finance and Accounting Directorate

SUBJECT: Draft Audit Report on Application Controls Over
               the Defense Joint Military Pay System Reserve
               Component (Project No. 6FD-2015)

Reference: DODIG Report, subject as above, 28 Apr 97

1. We have reviewed the subject draft report as per your request
and concur with the recommendations addressed to our Agency. The
review was conducted by DISA's Western Hemisphere (WESTHEM) and
detailed management comments are enclosed.

2. The point of contact for this action is Ms. Sandra J.
Sinkavitch, Audit Liaison, on (703) 607-6316 or electronic mail .
address sinkavis@ncr.disa.mil.

FOR THE DIRECTOR:

1 Enclosure a/s   RICHARD T. RACE
                                         Inspector General

Quality Information for a Strong Defense

40

DISA COMMENTS TO DODIG DRAFT AUDIT REPORT ON
Application Controls Over the Defense Joint Military Pay System
Reserve Component (Project No. 6FD-2015)

1. **Recommendation B.1.a:** Recommend Director, Defense Megacenter Denver improve the security for the DJMS by providing advance written notification of all security changes directly or indirectly affecting the DJMS to the Information System Security Officers, Directorate of Military Pay, DFAS-DE.

Comments: Concur with the recommendation. DMC Denver conducts weekly meetings, referred to as the configuration change request process, in which the DMC customers are present and have the ability to see and discuss upcoming security changes before they occur. As of 1 May 1997, DMC Denver has provided, and will continue to provide, written notification to the ISSO's, Directorate of Military Pay, DFAS-DE, of all security changes that directly or indirectly affect the DJMS. The action required by the recommendation is basically administrative and requires no technical changes or application. The DMC has incorporated this recommendation into their procedures; therefore, recommend closure of the recommendation.

2. **Recommendation B.1.b:** Recommend the Director, Defense Megacenter Denver improve the security for the DJMS by receiving approval from the Information System Security Officers, Directorate of Military Pay, DFAS-DE, before granting access to any Air Force DJMS resource.

Comments: Concur with the recommendation. The DMC Denver agrees with the recommendation to receive approval from the ISSO's before granting access to any Air Force DJMS, and as of 1 May 1997, any access granted by DMC Denver will first receive DFAS-DE ISSO approval. Complying with this recommendation is an administrative matter and requires no change to the DMCs current operating procedures. As 1 May 1997, the DMC has incorporated this recommendation into their procedures; therefore, recommend closure of the recommendation.

3. **Recommendation B.1.c:** Recommend the Director, Defense Megacenter Denver improve the security for the DJMS by reviewing the Customer Information and Control System command-level transactions for the individual DJMS production regions and limit access to these transactions to individuals with a need to know.

Enclosure

41

(Continuation of DISA Comments to DJMS (Project No. 6FD-2015))

Comment: Concur with the recommendation. DMC Denver completed a review of these sensitive CICS Owned Transactions (OTRANS), specifically *x* . DMC Denver needs to re-confirm with the functional user that the accesses are necessary and appropriate and have the required need-to-know. The user cannot execute a sensitive CICS OTRANS for a facility that the user does not have access to; in other words, a CICS user in another region cannot execute a command that will impact the DJMS CICS region. A further restriction to the user is enabled whereby the user can only execute the sensitive CICS OTRANS within a specifically designated facility. DMC Denver has identified several additional areas for review within the DMC and DFAS relating to the sensitive CICS OTRANS. This review and any necessary updates will be completed by 31 July 1997.

2

*Sensitive computer security information deleted (DoD 5400.7-R).

Audit Team Members

This report was produced by the Finance and Accounting Directorate, Office of the Assistant Inspector General for Auditing, DoD.

F. Jay Lane
David C. Funk
W. Andy Cooley
John W. Barklage
Frances E. Cain
Thomas G. Hare
Ben J. Meade
Deborah Curry

43

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Application Controls Over the Defense Joint Military Pay System Reserve Component

B. DATE Report Downloaded From the Internet: 10/13/99

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #):   **OAIG-AUD (ATTN: AFTS Audit Suggestions)**
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA   22202-2884

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ Preparation Date 10/13/99

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.